Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of determining a result of a group operation performed on a computing apparatus an integral number of times on a selected element of a [the] group having a plurality of elements including a group identity element, said method comprising the steps of:-

a) representing said integral number as a binary vector of bits having one value or another,

b) initialising [an intermediate value] said result to that of said group identity element;

c) selecting in sequence a predetermined number of successive bits [beginning with a left most bit]of said vector and for each of said selected bits;

i) performing said group operation on said result [intermediate element]to derive a [new] first intermediate [element] value,

ii) [replacing said intermediate element with said new intermediate element; iii)]obtaining a second intermediate value by performing said group operation on said first intermediate value [element] and [an] said selected element when said computing apparatus is in one state and by performing said group operation on said intermediate value and an inverse of said selected element when said computing apparatus is in another state [selected from the group consisting of ' said group element if said selected bit is a one; and an inverse element of said group element if said selected bit is a zero];

iii) replacing said result with said second intermediate value,

iv) [replacing said intermediate element with said new intermediate element] selecting a

state of said computing apparatus by examining an immediately preceding bit and maintaining the current state when said bits are of the same value and changing to said other state when said bits are different:

d) repeating step c) for said predetermined number of said bits and performing said group operation on any remaining bits of said vector, [d) performing said group operation on said intermediate value and said inverse element if said last selected bit is a zero; and replacing said intermediate element therewith, to obtain said result],whereby each of said predetermined bits of said of said vector is processed with substantially equal operations, thereby inhibiting disclosure of said sequence of predetermined bits [minimizing timing attacks on said cryptograhic system].

2. (currently amended) A method as defined in claim 1, said group being a multiplicateive group F_p* said group element being an integer, and said group operation being exponentiation g^a and [an] said inverse of said selected element [being] having a value corresponding to a [the] multiplicative inverse of said selected element [1/g].

3. (original) A method as defined in claim 1, said group being an additive group E (F_{2^m}) and said group operation being addition of points.

4. (currently amended) A method as defined in claim 1, said group being an additive group E (F_q), said group element being a point P with coordinates (x,y) on [the] an elliptic curve, and said group operation being [the] a scalar multiple kP of said point and an inverse element being [the] a negative –P of said point.

5. (currently amended) A method as defined in claim 1, said integral [value] number being a private key k used in a cryptosystem.

6. (currently amended) A method of performing a selected group operating on a scalar and a selected element of [said] a group having a plurality of elements, in a cryptographic processor, said method comprising the steps of:

representing said scalar as a binary vector;

recoding said binary vector to produce a signed digit representation of plus one and minus one digist;

selecting each of said [recoded bits] digits of said signed digit representation sequentially and for each of [said] the selected [bits] digits performing said group operating on an intermediate element to derive a new intermediate element; and adding or subtracting [said] a selected element of said group to said intermediate element in accordance with said signed digit representation [sign if said digit] being as each digit is selected; and

outputting said intermediate [value] element as a result of said group operation.

7. (new) A method according to claim 1 said group operation is performed on said result and said inverse of said selected element if said last of said predetermined bits is one of said values.

8. (new) A method according to claim 7 wherein said predetermined number of bits represents said entire vector.

9. (new) A method according to claim 8 wherein said one of said values is representative of zero.